FAA National Software Conference
CNS/ATM Guidelines

Guidelines for the Application of Software Development Assurance Best Practices to CNS/ATM Safety-critical Systems

Ron Stroup,
FAA, Office of Information Services
Process Engineering Division, AIO-200
(202) 494-4390
Ronald.L.Stroup@faa.gov
www.faa.gov/aio/

1

Work Began in May, 1998
Team members:

AWA	AIT-5 (AIO)
ANM	TRW-SETA
AOP	MITRE
ANS	ASD
AVA	AUATAC
AND	ASU
ASY	ASX
AIR	AOS

2

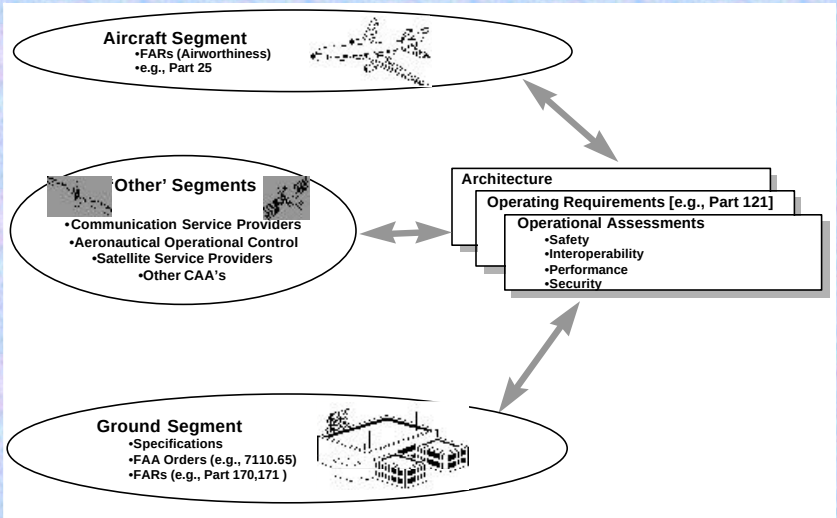
FAA National Software Conference
CNS/ATM Guidelines

Guidelines Schedule

- 9/1/99
  - Issued Initial working copy
- 9/1/00
  - Update based on experience and output of RTCA/SC-190
- 5/1/01
  - Issue initial release

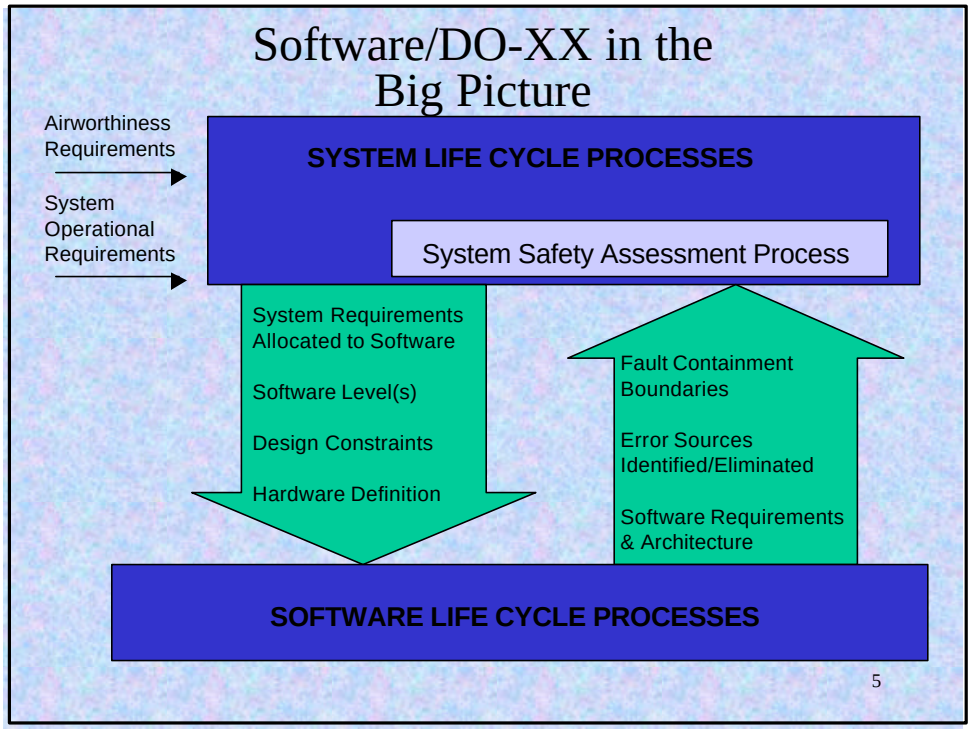
3

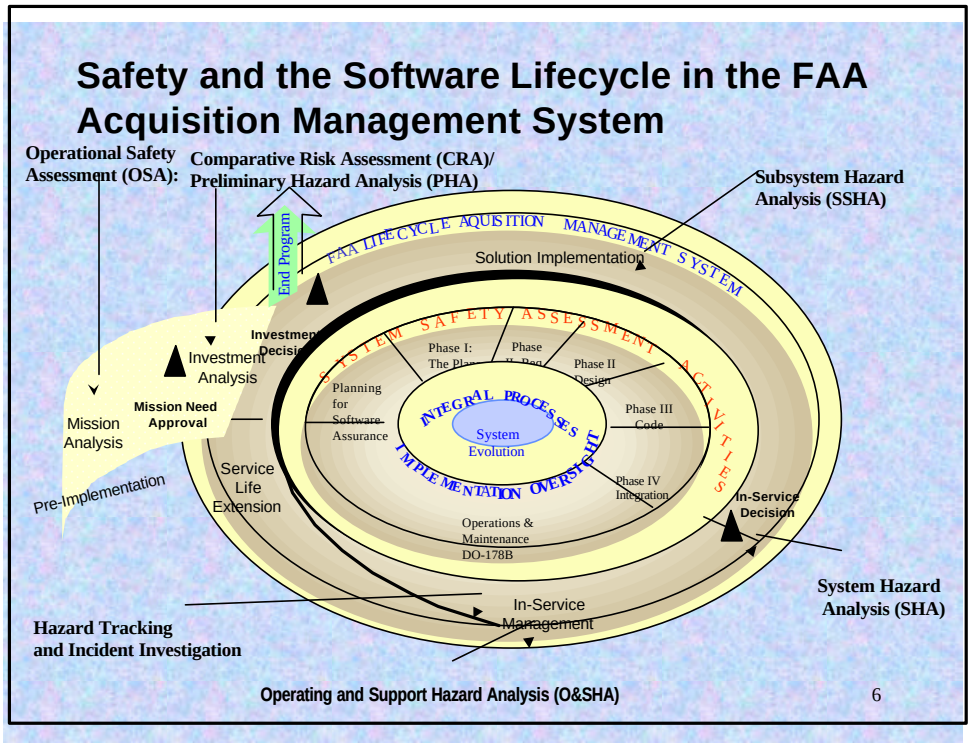
Purpose: to provide guidance to ensure consistency and an acceptable level of confidence in the development of software components of the NAS.



4

FAA National Software Conference
CNS/ATM Guidelines





FAA National Software Conference
CNS/ATM Guidelines

Assurance Activities

7

Mission Needs/Investment Analysis

- Contract planning
  - Safety, Security and Software Engineering should provide input.
  - Assess FAA capabilities to meet best overall solution.
  - Provide accurate cost and time estimates
  - Prepare Preliminary FHA
  - Prepare safety risk assessment

8

FAA National Software Conference
CNS/ATM Guidelines

Solution Implementation - Software Planning

- FAA
  - Complete system and subsystem hazard analysis
  - Ensure specifications are unambiguous, consistent, verifiable, and include assurance
  - Determine level of involvement
  - Plan to perform on-site reviews
- Supplier
  - Be knowledgeable of current software processes and standards
  - Discuss safety program and software levels
  - Identify special software considerations

9

Solution Implementation - Requirements

- FAA
  - Perform on-site reviews
  - Ensure SSA assumptions remain valid based on output from requirements process
  - Verify safety requirements allocated to software are present
  - Verify traceability from system requirements to software requirements
- Supplier
  - Follow approved plans and transition criteria
  - Coordinate any changes to process with FAA
  - Document evidence of design process compliance
  - Perform internal software reviews using FAA software job aid

10

FAA National Software Conference
CNS/ATM Guidelines

Solution Implementation - Design

- FAA
  - Perform on-site reviews per software job-aid
  - Ensure SSA assumptions are valid based on output of design process
  - Verify traceability from software requirements to design specification
  - Verify safety requirements have been met
  - Participate in CDR
- Supplier
  - Document evidence of design process compliance

11

Solution Implementation - Code Development

- FAA
  - Verify coding standards are being followed
  - Verify code is consistent with design specification
  - Verify traceability from code to requirements
  - Verify safety requirements have been met
- Supplier
  - Document code thoroughly
  - Follow coding standards
  - Perform code walk through or inspections

12

FAA National Software Conference
CNS/ATM Guidelines

Solution Implementation - Verification

- FAA
  - Participate in Test Readiness Review
  - Verify traceability between requirements, design, code, and test
  - Verify test procedures identify expected results
  - Ensure verification activities have been accomplished
  - Verify safety requirements have not been violated
- Supplier
  - Document verification and test results, including problems
  - Conduct software conformity review

13

Solution Implementation - Conformity review

- FAA
  - Address any open items from previous reviews and meetings
- Supplier
  - Document software problems and safety related issues
  - Coordinate with systems on safety issues

14

FAA National Software Conference
CNS/ATM Guidelines

In-Service Management/Service Life Extension

- FAA
  - Perform Change Impact analysis on modifications
  - Ensure safety requirements are remain valid
- Supplier
  - Identify new technologies when evaluating modifications

15

Tools

- Change Impact Analysis
- Level of FAA Involvement (LOFI)
- Software Job Aid

16

Change Impact Analysis

17

Change Impact Analysis

- Identify the software changes
- Determine effect of the change:
  - Traceability analysis
  - Memory/timing margin analysis
  - Data/Control flow analysis
  - Bus Loading
  - Requirements and design analysis
  - Code analysis
  - Development environment and process analysis
  - Test case analysis

18

FAA National Software Conference
CNS/ATM Guidelines

LOFI

19

Purpose

- Documents the criteria for determining when, the extent, and the areas in which FAA personnel should be involved in the software aspects of an acquisition program.

20

FAA National Software Conference
CNS/ATM Guidelines

Criteria

- Software Level
  - Level D LOW
  - Level C LOW or MEDIUM
  - Level B LOW or MEDIUM or HIGH
  - Level A MEDIUM or HIGH
- Other Relevant Criteria
  - Software Experience
  - Software Development Capability
  - Developers Service History
  - Current Software Applications

21

Level Attributes

- HIGH
  - Minimum 2 on-site reviews
  - Submittal of plans (SDP, SVP, SCMP, SQAP, SAS)
  - Submittal of compliance matrix
- MEDIUM
  - Minimum of 1 on-site review (mostly desk reviews)
  - Submittal of plans (SCI, SAS)
- LOW
  - Minimum desk reviews
  - Submittal of plans (SCI, SAS)

22

Software Job-Aid

23

Purpose of the Job Aid

- Standardize the Software Review Approach
- Provide a Tool for Engineers to Perform the Software Review (as a team)
- Improve the Quality of Software Reviews
- Inform Applicants of the FAA's Approach

24

Some Considerations When Using the Job Aid

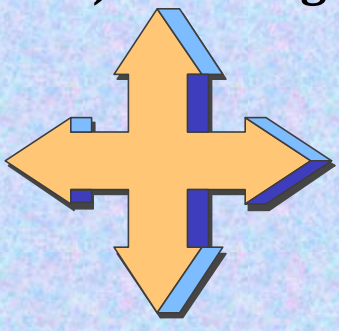
- Do Not Use as a "Checklist"
- Use with DO-178B
- Tailor as Needed
- Provide Feedback for Future Updates

25

Four Stages of Involvement

1) Planning

4) Final



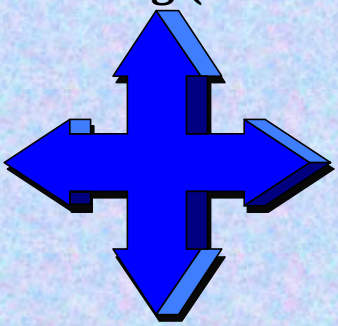
2) Development

3) Verification/Test

26

Four Stages of Involvement & Relationship to DO-178B

1) Planning (A-1/A-8/A-9/A-10)



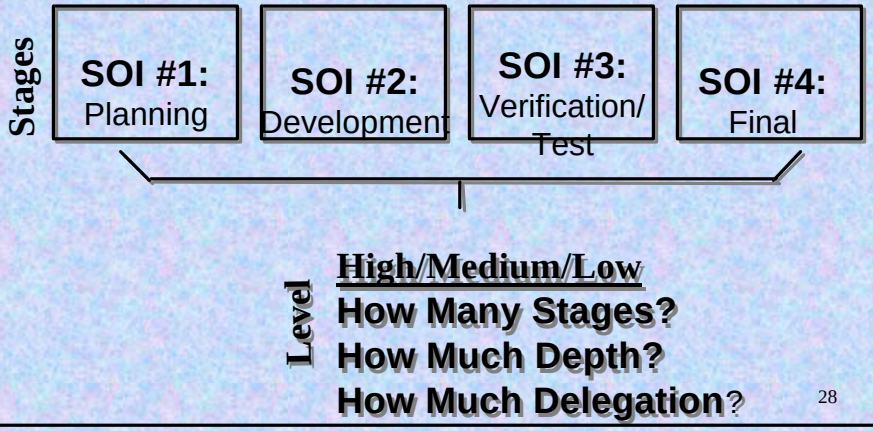
4) Final (All)

2) Development (A-2/A-3/A-4/A-5/ A-6/A-8/A-9/A-10)

3) Verification/Test (A-7/A-8/A-9/A-10)

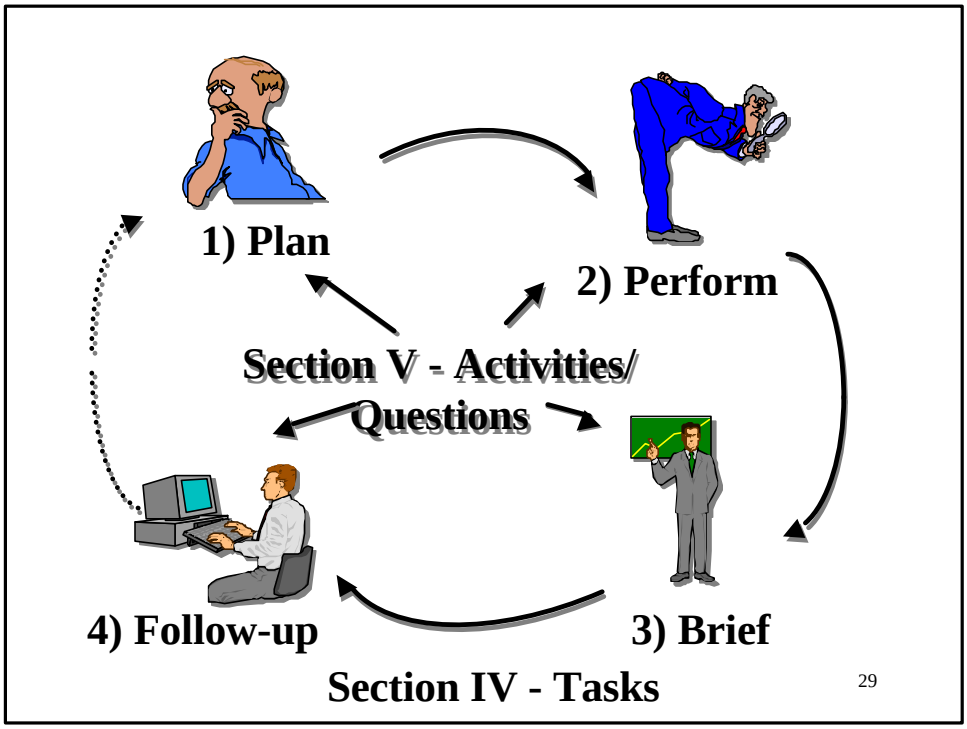
27

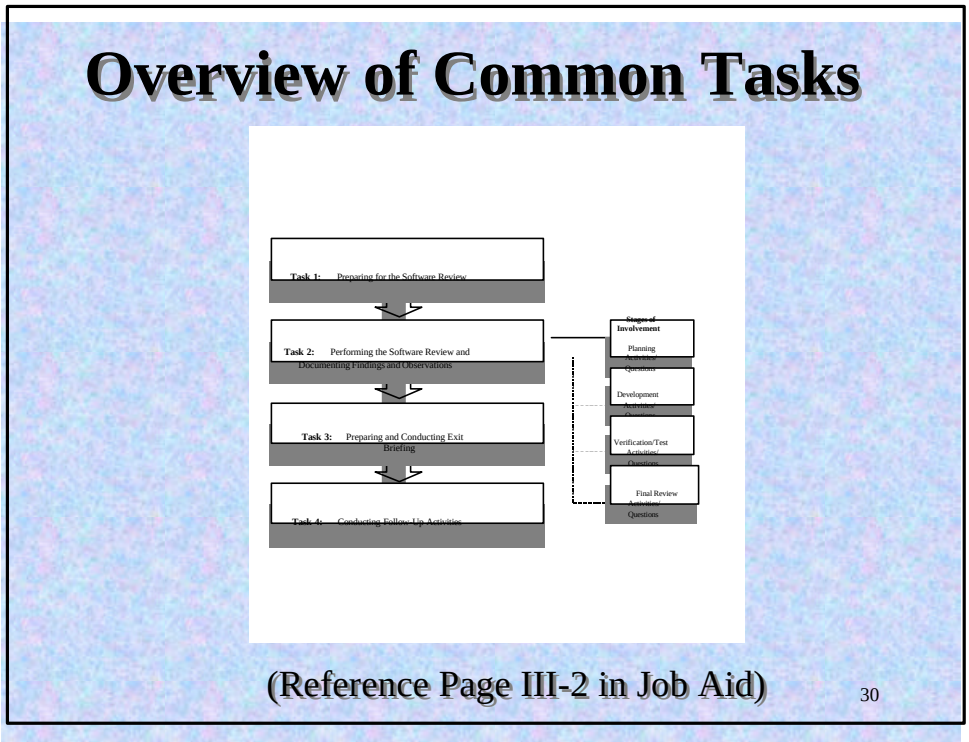
Stages versus Levels



28

FAA National Software Conference
CNS/ATM Guidelines





Review Tips

- **Communicate with Team Members**
- **Work Efficiently**
- **Be Considerate and Cooperative**
- **Be Flexible**
- **Allow the Data to Speak for Itself**

31

Tailoring the Job Aid (1/2)

- Prior to Review, Evaluate Activities/ Questions
- Delegate Activities/ Questions to Designees, as Appropriate
- Add Activities/Questions, as Appropriate
- Delete Activities/Questions, as Appropriate

32

Tailoring the Job Aid (2/2)

- **During the Review, the Situation May Lead to a Change in Direction**
- **Job Aid is Designed For Flexibility**
- **Job Aid is NOT A CHECKLIST**

33

Summary

- Outlines Best Practices for applying DO-178B to CNS/ATM systems.
- Identifies Tools to support the use of DO-178B
  - Change Impact Analysis
  - Level of FAA Involvement
  - Job-aid
- Can be viewed on the internet
- Comments accepted via Email

34